State of Utah
GARY R. HERBERT
Governor
GREG BELL
Lieutenant Governor

Department of Technology Services
J. STEPHEN FLETCHER
CIO
Executive Director

May 10, 2012

Purita G. Buck
Bureau of Medicaid Operations
Operation Support & Development

Ms Buck,

In response to your inquiry, related to security measures taken by the Department of Technology Services after the Medicaid records data breach I offer the following:

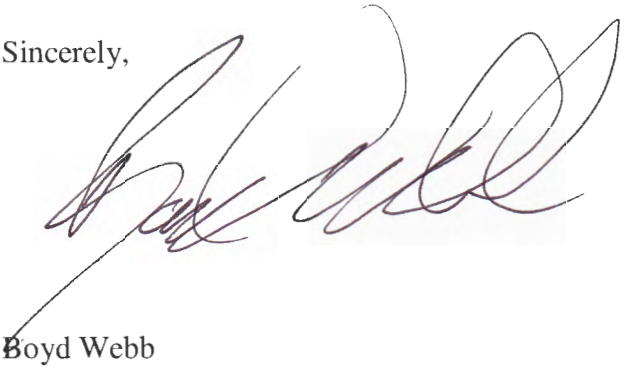
1. All servers used by the Department of Health have been audited to ensure that strong passwords and authentication is properly implemented.
2. All administrative passwords used to access servers hosting Health Department data have been changed.
3. All servers used by the Department of Health have been audited for exploit vulnerabilities using the Metasploit Professional and Nexpose Enterprise assessment products.
4. Application layer data encryption has been programmatically implemented into the process application to ensure that data stored on the server is encrypted in transit and at rest.
5. The Department of Technology Services, Office of Enterprise Security, has reviewed all relevant security policies with key management personnel and technical staff assigned to support the Health Department.
6. The Department of Technology Services, Office of Enterprise Security enhanced continuous threat monitoring capabilities, including the acquisition and training of additional staff.
7. The Department of Technology Services, Office of Enterprise Security implemented "Next Generation" network monitoring tools and processes to enhance rapid detection and attack mitigation capabilities.

Issues specific to the new Medicaid 5010 eligibility server have been addressed as indicated in the report included with this letter, which demonstrates that no critical vulnerabilities were discovered during the audit. A single vulnerability classified as "severe" in the audit report is a false positive related to the Secure Socket Layer (SSL) encryption key strength which is currently established at 128 bit. The Nexpose vulnerability assessment product ranks SSL encryption key strength less than 256 bit as a severe vulnerability. 128 bit encryption key strength is in compliance with Federal Information Processing Standards (FIPS) 142.

I personally certify that the remediation measures described above have been validated by the Department of Technology Services, Office of Enterprise Security.

Please feel free to contact me with additional questions and/or concerns.

Sincerely,



Boyd Webb
CISO
State of Utah,
Department of Technology Services